

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

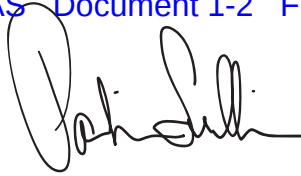
I, Craig A. Graham, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with Federal Bureau of Investigation (FBI), and am assigned to the Boston Field Office, Providence, RI. I have been an FBI agent since 2010. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, including but not limited to, violations of 18 U.S.C. §§ 2422, 2251, 2252, and 2252A. I have received training in the investigation of internet crime, child exploitation, transportation of minors, and child sexual abuse, and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256).

2. I am currently participating in an investigation relating to violations of federal law by NEIL STREICH for attempted transfer of obscene material to a minor, in violation of 18 U.S.C. § 1470; attempted enticement, coercion or persuasion of a minor to engage in prohibited sexual activity by means of a facility of interstate commerce, in violation of 18 U.S.C. § 2422(b)), and the possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4). This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this Affidavit, including the entire property located at [REDACTED] (the “SUBJECT PREMISES”), the content of electronic storage devices located therein,

"Person of Neil Streich"



~~Any person~~ located at the SUBJECT PREMISES, for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1470, 2422, and 2252, which items are more specifically described in **Attachment B** of this Affidavit.

3. The statements in this affidavit are based in part on information provided by FBI Agents in the FBI Philadelphia Division, Pennsylvania, and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1470 (attempted transfer of obscene material to a person under age 16); 18 U.S.C. § 2422(b) (use of means of interstate or foreign commerce to persuade, entice, or coerce a minor to engage in explicit sexual activity; and 18 U.S.C. §§ 2252(a)(4)(B) (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct), are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:
- a. Title 18, United States Code, Section 1470 prohibits any person from using a means of facility of interstate commerce to knowingly transfer obscene material to another individual who has not attained 16 years of age, or attempting to do so;
 - b. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, [...] matter which contain any

visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. Title 18, United States Code, Section 2422(b) prohibits any person from using a means of interstate or foreign commerce to persuade, induce, entice, or coerce any person under the age of eighteen to engage in sexual activity for which any person can be charged with an offense, or attempting to do so.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Chat room,” as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

c. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

d. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image of picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

f. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes,

and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

g. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. “Hashtag,” as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service

Providers (ISPs) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

j. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

k. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

m. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

n. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

o. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

p. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

q. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, thumb drives, and other magnetic or optical media.

r. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

s. “Obscene material” is any image or video representation containing material which the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; depicts in a patently

offensive way, sexual conduct and taken as a whole, lacks serious literary, artistic, political, or scientific value such as patently offensive representations or descriptions of ultimate sexual acts, normal or perverted, actual or simulated, patently offensive representation or descriptions of masturbation, excretory functions, and lewd exhibition of the genitals. Based on my training and experience, I am aware that Courts have upheld convictions of defendants for transferring obscene material to a minor under age 16 in violation of 18 U.S.C. § 1470 in instances where the defendant sent videos or images of his erect penis and/or videos or images of an adult male masturbating See e.g., United States v. Vasquez-Rivera, 665 F.3d 351, 354 (1st Cir. 2011) (defendant convicted of 18 U.S.C. § 1470 at trial, for sending a webcam video of a man masturbating); United States v. Madera-Ortiz, 637 F.3d 26 (1st Cir. 2011) (defendant convicted by guilty plea of 18 U.S.C. § 1470, after sending webcam footage that showed him touching his genitals and masturbating during chats with an u/c); United States v. Gravenhorst, 377 F.3d 49 (1st Cir. 2004), (defendant convicted on possession of child pornography charges, and transmission of obscene material to a minor for sending “sexually-charged images, including a picture of a man and woman having intercourse and a picture of an erect penis”), vacated on other grounds, 544 U.S. 1029 (2004) (vacated following the Booker ruling); United States v. Crespo-Rios, 2015 WL 6394256 (D. P.R. 2015); (defendant convicted of 18 U.S.C. § 1470 for sending a picture of his bare, erect penis).

PROBABLE CAUSE

6. Based on my training and experience and other investigations I have participated in, I am aware that there is subculture referred to as “daddy/princess” or variants thereof, which

consists of adult men who have sexual and romantic interest in minor females. In this subculture, the adult man will often play the role of “daddy” and the minor female of “princess.” There are groups and chat rooms on the internet where “daddies” and “princesses” can meet to exchange communication, videos and images. I am aware that many sexual predators exploit this subculture as a means of grooming minors to engage in illicit sexual activity, including producing sexually explicit images of themselves, and sometimes meeting in person for illicit sexual activity. The relationships can become coercive, as the “princess” is required to follow the instructions of the “daddy.” Often times the “daddy will instruct the “princess” not to tell her parents about the existence of their relationship, and will assume the role of surrogate parent by listening to the minor’s problems and offering advice, developing trust over time which can later be sexually exploited. Based on my training and experience it is not uncommon for “daddy/princess” relationships to develop over an extended period of time to include weeks or months before escalating to explicit sexual conduct.

7. On March 21, 2020, an undercover law enforcement officer, operating as a 10 year-old female, received an unsolicited message from [REDACTED] vanity name “Robert (straight daddy)”, username “rob.s063”. “rob.s063” stated that they were previously on a [REDACTED] group involving “daddy’s” and “princesses”. The undercover officer had previously been operating in a group which approximated the words “daddy’s” and “princesses” in its name.
8. During the conversation between “rob.s063” and the undercover officer, the undercover officer identified themselves as “10f from pa” meaning a 10 year-old female from Pennsylvania. When discussing what the undercover officer looked like, the undercover

officer again stated that they were only 10 years-old. The UC described “herself” as “4’9 thin brown hair and eyes no boobies.” “rob.s063” replied “I love that tiny no boobs is that really what you look like or is that what you used to look like when you were much younger [smile emoji].” The UC replied “LOL no that’s me. I’m only 10 so like negative a boobs.” “rob.s063” replied “well I’ve never been a boob fan I like pretty eyes and a cute round ass.”

9. “rob.s063” continued to express skepticism that the undercover officer was 10 years-old and requested “can I see a live pic because I’ve never met anyone on [REDACTED] who is under 15.”
10. On March 24, 2020 the UC sent a non-sexually explicit image that appears to depict a minor child in a seated position with the point of view at her legs with her swimsuit bottom on the ground between her legs. The image was not of a real child. “rob.s063” responded “Mmmmm cross your fingers in pic” and then “same pic.” The UC replied “WDYM [what do you mean] same pic?” to prove that the undercover was in fact a young girl. “rob.s063” sent the following message: “Just making sure your a younger girl so if you cross your fingers I’ll never question u again deal.” Over the next several days, “rob.s063” continued to request “pics” from the UC.
11. On March 27, 2020, the UC sent a non-sexually explicit image that appears to depict the torso of a young girl in a sun dress with her fingers crossed in front of her groin area with the message “here daddy”. The image was not of a real child. “rob.s063” responded by sending numerous pictures and videos of his erect penis and himself masturbating. “rob.s063” also stated “you do delete the pictures right don’t want parents finding.” “rob.s063” also stated “show me another pic of you in that dress nothing dirty... I could probably reach my hand around those young sexy thighs mmm.” In response, the UC sent another non-sexually

explicit image that appears to depict the torso of a young girl in a sun dress. The image was not of a real child. “rob.s063” continued to send sexually explicit images and videos of an adult male erect penis.

12. The conversation between “rob.s063” and the undercover officer lasted from March 21, 2020 to April 10, 2020. During that time “rob.s063” sent multiple videos of an erect penis as well as a video of himself masturbating while saying a name given by the undercover officer. “rob.s063” also changed his [REDACTED] vanity name to “Robert (taken)” to reflect that he and the undercover officer were now dating.

13. “rob.s063” identified himself as being from Connecticut, and having three children; a 24 year-old daughter, a 21 year-old son, and a 15 year-old son.

14. “rob.s063” also stated that he had previously been the “daddy” to a 16 year-old girl for three years before visiting her.

15. On April 28, 2020, MediaLab, Inc., the owner of [REDACTED] responded to a subpoena for information related to account “rob.s063”. The response included the unconfirmed email address “[REDACTED]@gmail.com” and recent IP addresses “174.192.19.26” and “108.34.155.100”.

16. On May 5, 2020, Verizon wireless responded to a subpoena related to IP address “174.192.19.26”. Subscriber information was provided as the following:

Telephone number: [REDACTED]

Galaxy Fasteners Inc., [REDACTED]

Subscriber Name: Mark Streich

17. On May 8, 2020, Verizon responded to a subpoena related to IP address “108.34.155.100”.

Subscriber information was provided as the following:

Daytime Telephone: [REDACTED]

Account Address: [REDACTED]

Customer Name: Neil Streich

Primary Telephone: [REDACTED]

Email Address: [REDACTED]@gmail.com

18. A check of publicly available databases revealed that Neil Streich, YOB 1963 resides at the SUBJECT PREMISES. A review of social media associated with Neil Streich indicated that he appeared to have children of same approximate age as those mentioned by account “rob.s063.”

19. A driver’s license for Neil Streich was reviewed and the SUBJECT PREMISES is listed on the license. Neil Streich’s driver’s license photograph was compared to the videos that “rob.s063” sent the undercover officer and it appeared that the person in the videos is Neil Streich. By contrast, Mark Streich’s driver’s license photograph was also compared to the videos that “rob.s063” sent and appeared to be a different person, who may be sibling of Neil Streich. In addition, based on my review of publicly available databases, I am aware that Neil Streich’s father, Robert, died in 1996. Based on all of the above, I believe that “rob.s063” is Neil Streich.

20. I am aware, based on my training and experience and other investigations I have participated in, that individuals who have a sexual interest in minor children will sometimes attempt to groom the minor child for sexual activity. This grooming activity can take a variety of

forms, including communicating in chat rooms, such as “daddy/princess” subculture chat rooms; sending gifts; role playing; the exchange of sexually explicit videos and images, the exchange of erotic but non-sexually explicit images and videos; flattery and controlling behavior and plans to meet. I am also aware that such individuals often share an interest in child pornography, including images and videos they obtain via the internet and images and videos obtained from minors with whom they have communicated online.

21. Based on my review of the evidence outlined herein, including but not limited to the sexually explicit material sent by “rob.s063” to the UC, his solicitation of images from the UC, his change of status to “taken” as well as his statements that he previously was a “daddy” to a 16 year old girl for 3 years before visiting her, I believe there is probable cause that NEIL STREICH has committed the offense of attempted transfer obscene material to a minor and attempted enticement of a minor to engage in illicit sexual activity. In addition, notwithstanding “rob.s063”’s directive to the UC not to send “dirty” pictures, I believe there is probable cause to believe that STREICH possesses child pornography on one or more electronic devices which he controls. This belief is based on my training and experience investigating people with a sexual interest in children. Such people often maintain collections of child pornography as well as child erotica. In addition, I am aware that in addition to chat groups dedicated to subcultures such as “daddy/princess” there are other chat groups on [REDACTED] which have been known by myself and other in law enforcement to be forums where individuals trade child pornography. Based on my training and experience, I believe there is a high likelihood that STREICH, who has a demonstrated sexual interest in minor children as young as at least 10 years old, likely possesses or accesses with intent to view

child pornography. Accordingly, this search warrant requests authorization to search for evidence of child pornography as well as enticement of a minor and transfer of obscene material to a minor.

22. Surveillance of the SUBJECT PREMISES on or about June 8, 2020 revealed that the number “41” is clearly marked on the front door of the house.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

23. I have had both training and experience in the investigation of computer-related crimes.

Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers

around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child

pornography can be found on the user's computer, smartphone or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

24. As described above and in Attachment B, this application seeks permission to search for records that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).
25. I submit that if a computer or storage medium, including a smart phone, is found at the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

26. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the SUBJECT PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the

innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data

typically also contains information indicating when the file or image was created.

The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
 - f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.
27. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard

drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

- a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;
- b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate

analysis of the equipment and storage devices from which the data will be extracted;

- c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and
- d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

28. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide

valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

29. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO ADVERTISE, TRANSPORT,
DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW
CHILD PORNOGRAPHY**

30. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

- a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.
- b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location.

Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Based on my training and experience, it is typical of individuals involved in child pornography to be initially reluctant to admit possessing child pornography or be willing to share such materials with other individuals on-line and to falsely and or inaccurately claim they deleted “all” of their child pornography collections. Often times such individuals maintain child pornography on a variety of different media and continue to keep child pornography even when some such materials are “deleted”. This is particularly true of individuals who have distributed child pornography in the past.

e. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor’s residence, inside the possessor’s vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

f. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals’ computers and digital

devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual “deleted” it.¹

g. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

h. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if an individual uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A.

¹ See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because “staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology”); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

REQUEST FOR SEALING

31. It is respectfully requested that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the SUBJECT PREMISES). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through forums. Premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on this continuing investigation and may jeopardize its effectiveness by alerting potential targets to the existence and nature of the investigation, thereby giving them an opportunity to flee, or to destroy or tamper with evidence.

CONCLUSION

32. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.
33. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

BIOMETRICS

34. The search warrant I am applying for would permit law enforcement to compel the use of NEIL STREICH’s biometric features. I seek this authority based on the following:
- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices—particularly newer mobile devices and laptops—offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features.

Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to use.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain

Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this affidavit, based on my training and experience, I believe that one or more digital devices will be found during the search. Further based on my training and experience, law enforcement personnel may not be able to fully execute the search authorized by this search warrant and thereby access the data contained within such device(s) without the use of biometric features.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device

manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for eight hours and the passcode or password has not been entered in the last six days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. In my training and experience, the person(s) who is or are in possession of a device or has the device among his or her belongings or at his or her premises at the time the device is found is likely to be a user of the device.

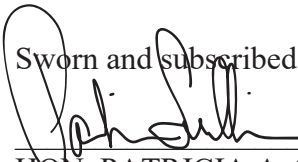
i. Due to the foregoing, if law enforcement personnel encounter device(s) that is or are subject to seizure pursuant to this search warrant and may be unlocked using one of the aforementioned biometric features, the search warrant I am applying for would permit law enforcement personnel, acting as soon as reasonably practicable, to compel the following: (1) press or swipe the fingers (including thumbs) of NEIL STREICH to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the

face of NEIL STREICH and activate the facial recognition feature; and/or (3)
hold the device(s) found at the premises in front of NEIL STREICH and activate
the iris recognition feature, for the purpose of attempting to unlock the device(s)
in order to search the contents as authorized by this search warrant.



Craig A. Graham
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 16th day of June, 2020.



HON. PATRICIA A. SULLIVAN
UNITED STATES MAGISTRATE JUDGE

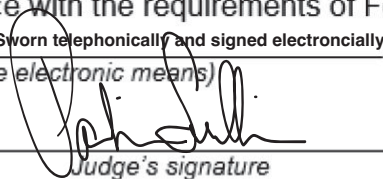
Attested to by the applicant in accordance with the requirements of Fed.
R. Crim. P. 4.1 by telephone Sworn telephonically and signed electronically.
(specify reliable electronic means)

June 16, 2020

Date

Barrington

R.I. *City and State*



Patricia A. Sullivan, US Magistrate Judge

Printed name and title

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The person of Neil Streich, a white male, born in 1963.

B. The content of any electronic media storage devices or media located on the person of Neil Streich or found in the premises of [REDACTED]
[REDACTED] Providence, RI 02909.

The entire property located at [REDACTED] including the residential building, any outbuildings, and any appurtenances thereto (the SUBJECT PREMISES). The building is a single family home, with a brick exterior and white trim. The number “41” is clearly affixed to the front door of the building.



Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by <u>telephone</u> <small>Sworn telephonically and signed electronically</small> <small>(specify reliable electronic means)</small>	
<u>June 16, 2020</u> <small>Date</small>	<u>[Signature]</u> <small>Judge's signature</small>
<u>Barrington</u> <u>R.I.</u> <small>City and State</small>	<u>US Magistrate Judge</u> <small>Printed name and title</small>

ATTACHMENT B

DESCRIPTION OF INFORMATION TO BE SEIZED

- I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. §§ 1470, 2422 and 2252, including:
 - A. Records and tangible objects pertaining to the following topics:
 1. Obscene materials;
 2. Child pornography and child erotica.
 3. Communications with minors or others having access to minors that relate to the persuasion, inducement, enticement or coercion of a minor to engage in sexual activity for which any person could be charged with a criminal offence.
 - B. For any electronic media storage device, computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant (“the computer equipment”):
 1. evidence of who used, owned, or controlled the computer equipment;
 2. Records and information showing access to and/or use of [REDACTED]
 3. Records and information relating or pertaining to the identity of the person or persons using or associated with “rob.s063.
 4. evidence of computer software that would allow others to control the items, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious

software;

5. evidence of the attachment of other computer hardware or storage media;
6. evidence of counter forensic programs and associated data that are designed to eliminate data;
7. evidence of the times the computer equipment was used;
8. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;
9. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media; and
10. evidence indicating the computer user's state of mind as it relates to the crime under investigation.

C. Records and tangible objects relating to the ownership, occupancy, or use of the SUBJECT PREMISES (such as utility bills, phone bills, rent payments, mortgage payments, photographs, insurance documentation, receipts and check registers); and

D. records, information, and items relating to the ownership or use of computer equipment and other electronic storage devices found in or on the SUBJECT PREMISES, including sales receipts, bills for Internet access, and handwritten notes.

II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items

described in Paragraph I.

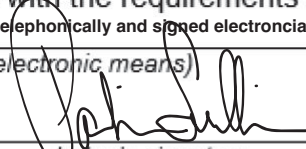
DEFINITIONS

For the purpose of this warrant:

- A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.
- B. "Computer hardware" means any electronic device capable of data processing (such as a computer, smartphone, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.
- D. "Computer related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- F. "Data" means all information stored on storage media of any form in any storage

format and for any purpose.

- G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.
- H. "Obscene material" is any image or video representation containing material which the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; depicts in a patently offensive way, sexual conduct and taken as a whole, lacks serious literary, artistic, political, or scientific value such as patently offensive representations or descriptions of ultimate sexual acts, normal or perverted, actual or simulated, patently offensive representation or descriptions of masturbation, excretory functions, and lewd exhibition of the genitals.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by <u>telephone</u> <small>Sworn telephonically and signed electronically</small> <small>(specify reliable electronic means)</small>	
<u>June 16, 2020</u> <small>Date</small>	 <small>Judge's signature</small>
<u>Barrington</u> <u>R.I.</u> <small>City and State</small>	<u>Patricia A. Sullivan, US Magistrate Judge</u> <small>Printed name and title</small>